IN THE CLAIMS:

1   1.   (Original) An elliptic curve arithmetic operation device for performing one of an

2   addition and a doubling on an elliptic curve $E: y\{2=f(x)$ on a residue class ring of polynomials

3   in two variables α and β, moduli of the residue class ring being polynomials $\beta\{2\text{-}f(\alpha)$ and $h(\alpha)$,

4   where $f(\alpha)=\alpha\{3+a\alpha+b$, a and b are constants, and $h(\alpha)$ is a polynomial in the variable α, the

5   elliptic curve arithmetic operation device comprising:

6   acquiring means for acquiring affine coordinates of at least one point on the

7   elliptic curve E and operation information indicating one of the addition and the doubling, from

8   an external source;

9   transforming means for performing a coordinate transformation on the acquired

10   affine coordinates to generate Jacobian coordinates, the coordinate transformation being

11   transforming affine coordinates $(\phi(\alpha), \beta x \varphi,(\alpha))$ of a given point on the elliptic curve E using

12   polynomials

13               $X(\alpha)=f(\alpha)\,x\phi(\alpha)$

14               $Y(\alpha)=f(\alpha)\{2x\varphi(\alpha)$

15               $Z(\alpha)=1$

16   into Jacobian coordinates $(X(\alpha):Y(\alpha):\beta x Z(\alpha))$, $\phi(\alpha)$ and $\varphi(\alpha)$ being

17   polynomials; and

18   operating means for performing one of the addition and the doubling indicated by

19   the acquired operation information, on the generated Jacobian coordinates to obtain Jacobian

20   coordinates of a point on the elliptic curve E.

1   2.   (Original) The elliptic curve arithmetic operation device of Claim 1,

2   wherein the acquiring means

3   (a)   in a first case acquires affine coordinates of two different points on the

4   elliptic curve E and operation information indicating the addition, and

5   (b)   in a second case acquires affine coordinates of a single point on the elliptic

6   curve E and operation information indicating the doubling,

7   wherein the transforming means

8   (a)   in the first case performs the coordinate transformation on the acquired

9   affine coordinates of the two different points to generate Jacobian coordinates of the two

10   different points, and

11   (b)   in the second case performs the coordinate transformation on the acquired

12   affine coordinates of the single point to generate Jacobian coordinates of the single point, and

13   wherein the operating means

14   (a)   in the first case performs the addition indicated by the acquired operation

15   information on the generated Jacobian coordinates of the two different points to obtain the

16   Jacobian coordinates of the point on the elliptic curve E, and

17   (b)   in the second case performs the doubling indicated by the acquired

18   operation information on the generated Jacobian coordinates of the single point to obtain the

19   Jacobian coordinates of the point on the elliptic curve E.

1   3.   (Currently Amended) The elliptic curve arithmetic operation device of Claim 2,

2   wherein in the first case

3   the acquiring means acquires affine coordinates

4   ~~$(X1(\alpha), \beta \times Y1(\alpha))$~~ $\underline{(\phi_1(\alpha), \beta \times \varphi_1(\alpha))}$

5 ~~(X2(α), βxY2 (α))~~ $(\phi_2 (\alpha), \beta x \varphi_2(\alpha))$

6 of the two different points on the elliptic curve E and the operation information

7 indicating the addition,

8 the transforming means performs the coordinate transformation on the acquired

9 affine coordinates of the two different points to generate Jacobian coordinates

10 $(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$

11 $(X2(\alpha) : Y2(\alpha) : \beta x Z2 (\alpha))$

12 of the two different points, and

13 the operating means computes

14 $U1(\alpha) = X1(\alpha) \, x Z2(\alpha) \; \{ 2$

15 $U2(\alpha) = X2(\alpha) \, x Z1(\alpha) \; \{ 2$

16 $S1(\alpha) = Y1(\alpha) \, x Z2(\alpha) \; \{ 3$

17 $S2(\alpha) = Y2(\alpha) \, x Z1(\alpha) \; \{ 3$

18 $H(\alpha) = U2(\alpha) - U1(\alpha)$

19 $r(\alpha) = S2(\alpha) - S1(\alpha)$

20 and computes

21 $X3(\alpha) = -H(\alpha) \; \{ 3 - 2 x U1(\alpha) x H(\alpha) \; \{ 2 + r(\alpha) \; \{ 2$

22 $Y3(\alpha) = -S1(\alpha) \, x H(\alpha) \; \{ 3 + r (\alpha) \, x \, (U1(\alpha) x H(\alpha) \; \{ 2 - X3 (\alpha))$

23 $Z3(\alpha) = Z1(\alpha) \, x Z2(\alpha) \, x H(\alpha)$

24 to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta x Z3(\alpha)$ of the point on the elliptic

25 curve E.

1   4.   (Currently Amended) The elliptic curve arithmetic operation device of Claim 2,

2   wherein in the second case

3   the acquiring means acquires affine coordinates

4      $~~~~~~~~~(X1(\alpha), \beta{\times}Y1(\alpha))~~(\phi_1 (\alpha), \beta{\times}\varphi_1(\alpha))$

5   of the single point on the elliptic curve E and the operation information indicating

6 the doubling,

7   the transforming means performs the coordinate transformation on the acquired

8 affine coordinates of the single point to generate Jacobian coordinates

9      $(X1(\alpha) : Y1(\alpha) : \beta{\times}Z1(\alpha))$

10   of the single point, and

11   the operating means computes

12      $S(\alpha){=}4 \times X1(\alpha) \times Y1(\alpha)$ { 2

13      $M(\alpha){=}3 \times X1(\alpha)$ { $2{+}\alpha \times Z1(\alpha)$ { $4 \times f(\alpha)$ { 2

14      $T(\alpha){=}{-}2 \times S(\alpha){+}M(\alpha)$ { 2

15   and computes

16      $X3(\alpha){=}T(\alpha)$

17      $Y3(\alpha){=}{-}8 \times Y1(\alpha)$ { $4{+}M(\alpha) \times (S(\alpha){-}T(\alpha))$

18      $Z3(\alpha){=}2 \times Y1(\alpha) \times Z1(\alpha)$

19   to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta{\times}Z3(\alpha))$ of the point on the elliptic

20 curve E.

1   5.   (Currently Amended) The elliptic curve arithmetic operation device of Claim 2,

2   wherein the acquiring means

3   (a)   in the first case acquires affine coordinates

4   ~~$(X1(\alpha), \beta x Y1(\alpha))$~~ $(\phi_1(\alpha), \beta x \varphi_1(\alpha))$

5   ~~$(X2(\alpha), \beta x Y2(\alpha))$~~ $(\phi_2(\alpha), \beta x \varphi_2(\alpha))$

6   of the two different points on the elliptic curve E and the operation information

7   indicating the addition, and

8   (b)   in the second case acquires affine coordinates

9   ~~$(X1(\alpha), \beta x Y1(\alpha))$~~ $(\phi_1(\alpha), \beta x \varphi_1(\alpha))$

10   of the single point on the elliptic curve E and the operation information indicating

11   the doubling,

12   wherein the transforming means

13   (a)   in the first case performs the coordinate transformation on the acquired

14   affine coordinates of the two different points to generate Jacobian coordinates

15                      $(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$

16                      $(X2(\alpha) : Y2(\alpha) : \beta x Z2(\alpha))$

17   of the two different points, and

18   (b)   in the second case performs the coordinate transformation on the acquired

19   affine coordinates of the single point to generate Jacobian coordinates

20                      $(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$

21   of the single point, and

22   wherein the operating means

23   (a)   in the first case computes

24          $U1(\alpha) = X1(\alpha) x Z2(\alpha)$ { 2

25          $U2(\alpha) = X2(\alpha) x Z1(\alpha)$ { 2

26          $S1(\alpha) = Y1(\alpha) x Z2(\alpha)$ { 3

27          $S2(\alpha) = Y2(\alpha) x Z1(\alpha)$ { 3

28          $H(\alpha) = U2(\alpha) - U1(\alpha)$

29          $r(\alpha) = S2(\alpha) - S1(\alpha)$

30   and computes

31          $X3(\alpha) = -H(\alpha)$ { 3-2x$U1(\alpha)$x$H(\alpha)$ { 2+$r(\alpha)$ { 2

32          $Y3(\alpha) = -S1(\alpha)$x$H(\alpha)$ { 3+$r(\alpha)$x($U1(\alpha)$x$H(\alpha)$ { 2-$X3(\alpha)$)

33          $Z3(\alpha) = Z1(\alpha)$ x$Z2(\alpha)$x$H(\alpha)$

34   to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta x Z3(\alpha))$ of the point on the elliptic

35 curve E, and

36   (b)   in the second case computes

37          $S(\alpha) = 4xX1(\alpha)xY1(\alpha)$ { 2

38          $M(\alpha) = 3xX1(\alpha)$ { 2+αx$Z1(\alpha)$ { 4x$f(\alpha)$ { 2

39          $T(\alpha) = -2xS(\alpha)+M(\alpha)$ { 2

40   and computes

41          $X3(\alpha) = T(\alpha)$

42          $Y3(\alpha) = -8xY1(\alpha)$ { 4 +$M(\alpha)$x($S(\alpha) -T(\alpha)$)

43          $Z3(\alpha) = 2xY1(\alpha)xZ1(\alpha)$

44   to obtain the Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta x Z3(\alpha))$ of the point on the

45 elliptic curve E.

1   6.   (Original) An elliptic curve order computation device for computing an order of

2   an elliptic curve according to a Schoof-Elkies-Atkin algorithm, comprising the elliptic curve

3   arithmetic operation device of Claim 1.

1   7.   (Original) The elliptic curve order computation device of Claim 6 comprising the

2   elliptic curve arithmetic operation device of Claim 2.

1   8.   (Original) The elliptic curve order computation device of Claim 7 comprising the

2   elliptic curve arithmetic operation device of Claim 5.

1   9-22.   (Cancelled)

1   23.   (Currently Amended) An elliptic curve arithmetic operation method used in an

2   elliptic curve arithmetic operation device equipped with an acquiring means, a transforming

3   means, and an operating means, for performing one of an addition and a doubling on an elliptic

4   curve $E: y\{2=f(x)$ on a residue class ring of polynomials in two variables α and β, moduli of the

5   residue class ring being polynomials $\beta\{2-f(\alpha)$ and $h(\alpha)$, where $f(\alpha)=\alpha\{3+a\alpha+b$, a and b are

6   constants, and $h(\alpha)$ is a polynomial in the variable α, the elliptic curve arithmetic operation

7   method comprising:

8   an acquiring step performed by the acquiring means, for acquiring affine

9   coordinates of at least one point on the elliptic curve E and operation information indicating one

10   of the addition and the doubling, from an external source;

11   a transforming step performed by the transforming means, for performing a

12   coordinate transformation on the acquired affine coordinates to generate Jacobian coordinates,

13   the coordinate transformation being transforming affine coordinates $(\phi\,(\alpha),\ \beta x\varphi(\alpha))$ of a given

14   point on the elliptic curve E using polynomials

15                         $X(\alpha) = f(\alpha)x\phi\,(\alpha)$

16                         $Y(\alpha) = f(\alpha)\ \{\ 2x\varphi\,(\alpha)$

17                         $Z(\alpha) = 1$

18   into Jacobian coordinates $(X(\alpha)\ :Y(\alpha)\ :\beta xZ(\alpha))$, $\phi\,(\alpha)$ and $\not\phi\,(\not\alpha)$ $\underline{\varphi(\alpha)}$ being

19   polynomials; and

20   an operating step performed by the operating means, for performing one of the

21   addition and the doubling indicated by the acquired operation information, on the generated

22   Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve E.

1   24.   (Cancelled)

1   25.   (Original) A computer-readable storage medium storing an elliptic curve

2   arithmetic operation program used in an elliptic curve arithmetic operation device equipped with

3   acquiring means, transforming means, and operating means, for performing one of an addition

4   and a doubling on an elliptic curve $E:\ y\ \{\ 2=f(x)$ on a residue class ring of polynomials in two

5   variables α and β, moduli of the residue class ring being polynomials $\beta\ \{\ 2\text{-}f(\alpha)$ and $h(\alpha)$, where

6    $f(\alpha) = \alpha\ \{\ 3+a\alpha+b$, a and b are constants, and $h(\alpha)$ is a polynomial in the variable α, the elliptic

7   curve arithmetic operation program comprising:

8   an acquiring step performed by the acquiring means, for acquiring affine

9   coordinates of at least one point on the elliptic curve E and operation information indicating one

10   of the addition and the doubling, from an external source;

11   a transforming step performed by the transforming means, for performing a

12 coordinate transformation on the acquired affine coordinates to generate Jacobian coordinates,

13 the coordinate transformation being transforming affine coordinates $(\phi\,(\alpha),\ \beta x \varphi(\alpha))$ of a given

14 point on the elliptic curve E using polynomials

15    $$X(\alpha) = f(\alpha) x \phi\,(\alpha)$$

16    $$Y(\alpha) = f(\alpha)\ \{\ 2x\varphi\,(\alpha)$$

17    $$Z(\alpha) = 1$$

18   into Jacobian coordinates $(X(\alpha):Y(\alpha):\beta x Z(\alpha))$, $\phi\,(\alpha)$ and $\varphi\,(\alpha)$ being polynomials;

19 and

20   an operating step performed by the operating means, for performing one of the

21 addition and the doubling indicated by the acquired operation information, on the generated

22 Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve E.

1   26.   (Original) The storage medium of Claim 25, wherein the acquiring step

2   (a)   in a first case acquires affine coordinates of two different points on the

3 elliptic curve E and operation information indicating the addition, and

4   (b)   in a second case acquires affine coordinates of a single point on the elliptic

5 curve E and operation information indicating the doubling,

6   wherein the transforming step

7   (a)   in the first case performs the coordinate transformation on the acquired

8 affine coordinates of the two different points to generate Jacobian coordinates of the two

9 different points, and

10   (b)   in the second case performs the coordinate transformation on the acquired

11 affine coordinates of the single point to generate Jacobian coordinates of the single point, and

12   wherein the operating step

13   (a)   in the first case performs the addition indicated by the acquired operation

14 information on the generated Jacobian coordinates of the two different points to obtain the

15 Jacobian coordinates of the point on the elliptic curve E, and

16   (b)   in the second case performs the doubling indicated by the acquired

17 operation information on the generated Jacobian coordinates of the single point to obtain the

18 Jacobian coordinates of the point on the elliptic curve E.

1   27.   (Currently Amended) The storage medium of Claim 26, wherein in the first case

2 the acquiring step acquires affine coordinates

3   ~~$(X1(\alpha), \beta x Y1(\alpha))$~~ $(\phi_1(\alpha), \beta x \varphi_1(\alpha))$

4   ~~$(X2(\alpha), \beta x Y2(\alpha))$~~ $(\phi_2(\alpha), \beta x \varphi_2(\alpha))$

5   of the two different points on the elliptic curve E and the operation information

6 indicating the addition,

7   the transforming step performs the coordinate transformation on the acquired

8 affine coordinates of the two different points to generate Jacobian coordinates

9     $(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$

10    $(X2(\alpha) : Y2(\alpha) : \beta x Z2(\alpha))$

11   of the two different points, and

12   the operating step computes

13    $U1(\alpha) = X1(\alpha) x Z2(\alpha) \{ 2$

14    $U2(\alpha) = X2(\alpha) x Z1(\alpha) \{ 2$

15    $S1(\alpha) = Y1(\alpha) x Z2(\alpha) \{ 3$

16    $S2(\alpha) = Y2(\alpha) x Z1(\alpha) \{ 3$

17                 $H(\alpha) = U2(\alpha) - U1(\alpha)$

18                 $r(\alpha) = S2(\alpha) - S1(\alpha)$

19   and computes

20                 $X3(\alpha) = -H(\alpha) \{ 3-2xU1(\alpha)xH(\alpha) \{ 2+r(\alpha) \{ 2$

21                 $Y3(\alpha) = -S1(\alpha)xH(\alpha) \{ 3+r(\alpha)x(U1(\alpha)xH(\alpha) \{ 2-X3(\alpha))$

22                 $Z3(\alpha) = Z1(\alpha)xZ2(\alpha)xH(\alpha)$

23   to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta xZ3(\alpha))$ of the point on the elliptic

24 curve E.

1   28.   (Currently Amended) The storage medium of Claim 26,

2   wherein in the second case the acquiring step acquires affine coordinates

3                 $\cancel{(X1(\alpha), \beta xY1(\alpha))}$ $(\phi_1 (\alpha), \beta x\phi_1(\alpha))$

4   of the single point on the elliptic curve E and the operation information indicating

5 the doubling,

6   the transforming step performs the coordinate transformation on the acquired

7 affine coordinates of the single point to generate Jacobian coordinates

8                 $(X1(\alpha) : Y1(\alpha) : \beta xZ1(\alpha))$

9   of the single point, and

10   the operating step computes

11                 $S(\alpha) = 4xX1(\alpha)xY1(\alpha) \{ 2$

12                 $M(\alpha) = 3xX1(\alpha) \{ 2+axZ1(\alpha) \{ 4xf(\alpha) \{ 2$

13                 $T(\alpha) = -2xS(\alpha) +M(\alpha) \{ 2$

14   and computes

15          $X3(\alpha) = T(\alpha)$

16          $Y3(\alpha) = -8xY1(\alpha) \{ 4+M(\alpha)x(S(\alpha) -T(\alpha))$

17          $Z3(\alpha) = 2xY1(\alpha)xZ1(\alpha)$

18   to obtain Jacobian coordinates $(X3(\alpha) :Y3(\alpha) :\beta xZ3(\alpha))$ of the point on the elliptic

19 curve E.

1   29.   (Currently Amended) The storage medium of Claim 26,

2   wherein the acquiring step

3   (a)   in the first case acquires affine coordinates

4          $\sout{(X1(\alpha), \beta xY1(\alpha))}$ $\underline{(\phi_1(\alpha), \beta x\varphi_1(\alpha))}$

5          $\sout{(X2(\alpha), \beta xY2(\alpha))}$ $\underline{(\phi_2(\alpha), \beta x\varphi_2(\alpha))}$

6   of the two different points on the elliptic curve E and the operation information

7 indicating the addition, and

8   (b)   in the second case acquires affine coordinates

9          $\sout{(X1(\alpha), \beta xY1(\alpha))}$ $\underline{(\phi_1(\alpha), \beta x\varphi_1(\alpha))}$

10   of the single point on the elliptic curve E and the operation information indicating

11 the doubling,

12   wherein the transforming step

13   (a)   in the first case performs the coordinate transformation on the acquired

14 affine coordinates of the two different points to generate Jacobian coordinates

15          $(X1(\alpha) :Y1(\alpha) :\beta xZ1(\alpha))$

16          $(X2(\alpha) :Y2(\alpha) :\beta xZ2(\alpha))$

17   of the two different points, and

18   (b)   in the second case performs the coordinate transformation on the acquired

19   affine coordinates of the single point to generate Jacobian coordinates

20              $(X1(\alpha):Y1(\alpha):\beta xZ1(\alpha))$

21   of the single point, and

22   wherein the operating step

23   (a)   in the first case computes

24              $U1(\alpha)=X1(\alpha)xZ2(\alpha)\{2$

25              $U2(\alpha)=X2(\alpha)xZ1(\alpha)\{2$

26              $S1(\alpha)=Y1(\alpha)xZ2(\alpha)\{3$

27              $S2(\alpha)=Y2(\alpha)xZ1(\alpha)\{3$

28              $H(\alpha)=U2(\alpha)-U1(\alpha)$

29              $r(\alpha)=S2(\alpha)-S1(\alpha)$

30   and computes

31              $X3(\alpha)=-H(\alpha)\{3-2xU1(\alpha)xH(\alpha)\{2+r(\alpha)\{2$

32              $Y3(\alpha)=-S1(\alpha)xH(\alpha)\{3+r(\alpha)x(U1(\alpha)xH(\alpha)\{2-X3(\alpha))$

33              $Z3(\alpha)=Z1(\alpha)xZ2(\alpha)xH(\alpha)$

34   to obtain Jacobian coordinates $(X3(\alpha):Y3(\alpha):\beta xZ3(\alpha))$ of the point on the elliptic

35   curve E, and

36   (b)   in the second case computes

37              $S(\alpha)=4xX1(\alpha)xY1(\alpha)\{2$

38              $M(\alpha)=3xX1(\alpha)\{2+axZ1(\alpha)\{4xf(\alpha)\{2$

39              $T(\alpha)=-2xS(\alpha)+M(\alpha)\{2$

40   and computes

41         $X3(\alpha) = T(\alpha)$

42         $Y3(\alpha) = -8xY1(\alpha) \{ 4 + M(\alpha) x(S(\alpha) - T(\alpha))$

43         $Z3(\alpha) = 2xY1(\alpha)xZ1(\alpha)$

44   to obtain the Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta xZ3(\alpha))$ of the point on the

45   elliptic curve E.

1   30-33.   (Cancelled)